

UNITED STATES DISTRICT COURT

OCT 25 2018

for the
District of MarylandAT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address)
 Certain Electronic Devices)
)
) Case No.
)
)

18 - 2443 - ADC

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ Maryland
 (identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before _____

(not to exceed 14 days)

in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

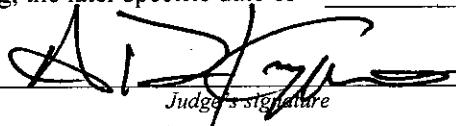
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for 30 days (not to exceed 30).

until, the facts justifying, the later specific date of _____.

Date and time issued:

5 September 2018 @ 10:00 AM

 Judge's signature

City and state: Baltimore, MD

Hon. A. David Copperthite, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

<i>Return</i>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
761055-16-0010		N/A
Inventory made in the presence of:		
<u>Special Agent Jessica Warner</u>		
Inventory of the property taken and name of any person(s) seized:		
<i>Electronic Evidence</i>		
<i>Certification</i>		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date:	<u>9/25/18</u>	
		Executing officer's signature
<u>G.T. Smith TFO</u>		Printed name and title

ATTACHMENT A

Description of the Items to be Searched

- A black Apple I-Phone (ATF Property number 31) (**Subject Electronic Device 1**);
- An Apple I-Phone (ATF Property number 38) (**Subject Electronic Device 5**);
- A black Apple I-Phone bearing IMEI number 990002287748766 (**Subject Electronic Device 7**);
- An Apple I-Phone bearing IMEI number 352006067031808 (**Subject Electronic Device 11**);
- An Apple I-Phone bearing IMEI number 35202606359836 (**Subject Electronic Device 12**);
- A black Apple I-Phone (ATF property number 61) (**Subject Electronic Device 19**);
- A pink Apple I-Phone (ATF property number 62) (**Subject Electronic Device 20**);
- A silver Apple I-Phone (IMEI 013884007360664) (**Subject Electronic Device 21**);
- A white Apple I-Phone bearing IMEI number 359300066793770 (**Subject Electronic Device 22**);
- A pink Apple I-Phone (ATF property number 97) (**Subject Electronic Device 25**)

The devices will be charged and powered on. The devices are in custody of the ATF and/or the Baltimore City Police Department. The devices and all readable and searchable contents will be downloaded to a “CelleBrite” or “XRY” or similar device. The contents downloaded on the “CelleBrite” or “XRY” or similar device will then be copied to a readable computer disc and reviewed by your affiant. A search warrant return will be provided to the Court thereafter.

ATTACHMENT B

Search Protocols

This warrant authorizes the search and seizure of the following electronically stored information, contained within the items described in Attachment A:

- a. digital images;
- b. digital videos;
- c. records of incoming and outgoing voice communications;
- d. records of incoming and outgoing text messages;
- e. the content of incoming and outgoing text messages;
- f. voicemails;
- g. voice recordings;
- h. contact lists;
- i. social media applications and the content of such applications;
- j. communication applications and the content of such applications;
- k. the content of device back-up accounts;
- l. records of web browser activity, history, and usage; and
- m. location data

that are related to the investigation into a drug trafficking conspiracy as more fully described in the Affidavit.

Because of the possibility that the files examined pursuant to the warrant will include information that is beyond the scope of what the United States has demonstrated the existence probable cause to search for, the search shall be conducted in a manner that will minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search is not viewed.

While this protocol does not prescribe the specific search protocol to be used, it does contain limitations to what the government investigators may view during their search, and the

searching investigators shall be obligated to document the search methodology used in the event that there is a subsequent challenge to the search that was conducted, pursuant to the following protocol.

With respect to the search of any digitally/electronically stored information that is seized pursuant to this warrant, and described in Attachment A hereto, the search procedure shall include such reasonably available techniques designed to minimize the chance that the government investigators conducting the search will view information that is beyond the scope for which the probable cause exists.

The following list of techniques is a non-exclusive list which illustrates the types of search methodology that may avoid an overbroad search, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein:

- a. Use of computer search methodology to conduct an examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether data falls within the items to be seized as set forth herein by specific date ranges, names of individuals, or organizations;
- b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;
- c. Physical examination of the storage device, including digitally surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein; and
- d. Opening or reading portions of files that are identified as a result of conducting digital search inquiries in order to determine their relevance.